p-ISSN: 2301-6949
e-ISSN : 2715-5064

Pengembangan Aplikasi Android PiGANO untuk Keamanan Pesan Menggunakan Kombinasi Caesar Cipher dan LSB

Muhammad Salam Pararta Saragi[1*)], Farhan Ramadhan Khoir[2], Muhammad Auriel[3], Rahmah Fauziah[4], Rajih Nibras Maulana[5], Syifa Aqila Humaira[6], Deden Pradeka[7], Zahra Khaerunnisa[8]
[1,2,3,4,5,6,7,8]Program Studi Teknik Komputer, Universitas Pendidikan Indonesia
[1,2,3,4,5,6,7,8]Jl. Dr. Setiabudhi No. 229, Isola, Kec. Sukasari, Kota Bandung, Indonesia
email: salam.sen@upi.edu[1], farhanramadhank7@upi.edu[2], iel.auriel25@upi.edu[3], rahmahfzh@upi.edu[4], rajihnmdx82@upi.edu[5], syifaqila@upi.edu[6], dedenpradeka@upi.edu[7], zahrakhae@upi.edu[8],

Abstrak **Keamanan data menjadi hal yang sangat penting untuk melindungi kerahasiaan dari seseorang. Keamanan dan kerahasiaan data berpengaruh terhadap proses pertukaran pesan penting. Banyak teknik keamanan data yang dapat digunakan demi menjaga kerahasiaan pesan dari pihak lain, meliputi kriptografi dan steganografi. Penelitian ini bertujuan mengembangkan aplikasi Android bernama PiGANO yang menggabungkan algoritma Caesar Cipher dan *Least significant bit* (LSB) guna meningkatkan keamanan dan kerahasiaan pesan dalam media gambar. Proses penelitian mencakup analisis kebutuhan, desain sistem, implementasi algoritma, serta pengujian aplikasi melalui tahapan perhitungan MSE dan PSNR dari hasil enkripsi untuk mengukur tingkat kesalahan dan kualitas gambar hasil enkripsi. Hasil penelitian menunjukkan bahwa aplikasi ini berhasil mengenkripsi pesan serta menyembunyikannya dalam media gambar dengan baik. Aplikasi ini memberikan tingkat keamanan ganda dengan memadukan teknik kriptografi dan steganografi, sehingga pesan terlindungi dari pihak yang tidak berwenang. Penerapan algoritma Caesar Cipher menghasilkan pesan yang terenkripsi dan sulit diakses, sementara algoritma LSB mampu menyembunyikan pesan dalam gambar digital tanpa mempengaruhi kualitas visual. Penelitian ini membuktikan bahwa kombinasi kedua teknik ini efektif untuk menjaga kerahasiaan data.**

Kata Kunci **– Kriptografi, Steganografi, Caesar Cipher, LSB, Android.**

I.PENDAHULUAN

Keamanan data menjadi hal yang penting untuk menjaga kerahasiaan dari seseorang, baik itu data pribadi maupun kelompok. Setiap kerahasiaan data tentunya bersifat sensitif dan memerlukan perlindungan yang kuat [1]. Keamanan dapat didefinisikan sebagai *"quality or state of being secure to be free from danger"* [2]. Maksudnya, suatu kondisi yang aman dan rahasia terkait data-data yang disimpan serta bebas dari bahaya yang mengancam. Untuk itu, keamanan dan kerahasiaan diperlukan dalam proses pertukaran pesan penting. Pada dasarnya, saat ini proses pertukaran belum menjamin bahwa pesan yang dikirimkan bebas dari pihak tidak berwenang sehingga diperlukan teknik keamanan data yang dapat melindungi isi pesan yang akan dikirimkan [3]. Sudah banyak teknik keamanan data yang berkembang demi menjaga kerahasiaan pesan dari pihak lain, meliputi kriptografi dan steganografi.

Kriptografi adalah ilmu yang mempelajari tentang tata cara melindungi keamanan pesan [4]. Dengan kriptografi pesan yang dikirimkan diubah menjadi bentuk kode yang tidak mudah diketahui, disebut sebagai proses enkripsi. Pada tahapannya, pesan yang dikirimkan diubah agar pihak ketiga tidak mengetahui isi pesan tersebut hingga ke pihak penerima [5]. Dalam hal ini, pihak penerima perlu melakukan pengubahan dari pesan yang tidak diketahui menjadi bentuk awal yaitu pesan yang diketahui. Perubahan yang dilakukan melalui proses dekripsi dengan mengembalikan isi pesan asli atau *plaintext* yang dimaksud agar dipahami oleh penerima [6]. Proses tersebut dilakukan menggunakan proses Caesar Cipher. Terdapat teknik lain yang dapat meningkatkan keamanan pesan. Steganografi adalah teknik yang digunakan dalam menyembunyikan pesan ke dalam bentuk media yang sulit diketahui [7]. Dengan steganografi maka dapat meminimalisirkan kecurigaan karena pesan yang disembunyikan berada dalam *file* pesan lain dan sangat sulit untuk diketahui secara langsung oleh panca-indra manusia. Biasanya media yang dapat digunakan dalam proses penyembunyian pesan meliputi gambar, teks, video, suara, dan sebagainya [8]. Hal tersebut sejalan dengan tujuan dari teknik steganografi supaya pihak lain tidak mudah mengidentifikasi pesan rahasia yang disisipkan di dalam media tersebut. Adapun kriteria dari steganografi meliputi proses yang tidak dikenali oleh indra manusia (*imperceptibility*), kualitas *file* yang tidak terlalu berbeda dengan yang asli (*fidelity*), dan *file* yang dapat diubah ke bentuk awal (*recovery*) [9]. Pada prosesnya menggunakan algoritma *Least Significant Bit* (LSB), menyembunyikan pesan dengan cara menyisipkan ke dalam barisan bit paling kanan yang ada di pixel *file* objek [10]. Teknik LSB dikenal menjadi teknik yang sederhana namun efektif dalam menyisipkan setiap informasi dalam bentuk citra digital [11]. Dalam penerapannya, bit yang sudah diubah oleh algoritma LSB akan disisipkan pada data yang lain, sehingga pesan yang tersembunyi dapat dikombinasikan tanpa mengubah strukturnya secara signifikan [12].

Tujuan dari penelitian ini untuk meningkatkan keamanan dan kerahasiaan pesan dalam media gambar, sehingga dilakukan pengembangan aplikasi Android bernama PiGANO dengan mengintegrasikan kombinasi antara teknik kriptografi dan steganografi. Prosesnya dengan memanfaatkan algoritma Caesar Cipher dan *Least significant bit* (LSB) merupakan teknik kriptografi dan steganografi yang digunakan dalam

prosedur penyembunyian pesan pada aplikasi ini. Kedua teknik ini memungkinkan pesan yang dikirim di enkripsi untuk menambah keamanan dan disembunyikan dalam bentuk media digital.

II.PENELITIAN YANG TERKAIT

1. Penelitian Terdahulu

Beberapa penelitian terkait pengembangan aplikasi Android menggunakan teknik kriptografi dan steganografi telah dilakukan sebelumnya. Penelitian yang dilakukan oleh Saifuddin mengenai pengembangan aplikasi steganografi berbasis Android menggunakan metode *Discrete Cosine Transformation* untuk pengamanan data. Pengujian menggunakan *Peak Signal to Noise Ratio* (PSNR) dan *Mean Square Error* (MSE). Hasil pengujian dengan menggunakan MSE menghasilkan rata-rata sebesar 0,472 dan pengujian dengan PSNR menghasilkan rata-rata 54.356 dB. Pada penelitian tersebut menunjukkan tidak terjadinya perubahan signifikan pada kualitas warna dari citra asli dengan citra steganografi, sehingga *file* yang disembunyikan tidak dapat dengan mudah untuk di deteksi oleh indra penglihatan manusia. Hal tersebut membuktikan bahwa proses pengamanan data berhasil diintegrasikan tanpa membuat pihak lain dapat mengetahuinya [13].

Penelitian lain yang dilakukan Nidia Enjelita Saragih mengenai penerapan kriptografi menggunakan algoritma *One Time Pad* berbasis Android untuk mengamankan isi *diary*. Dalam penelitiannya, melakukan perubahan *plaintext* menjadi ke *ciphertext*, kemudian diintegrasikan pada aplikasi Android. Pengujian dilakukan berdasarkan *plaintext*, kunci, hasil enkripsi dan dekripsi yang telah dibuat. Hal tersebut menunjukkan bahwa aspek kerahasiaan pesan *diary* yang dihasilkan dari proses enkripsi tidak sama dengan pesan asli, sistem menjamin keamanan data yang disimpan [14].

Penelitian yang dilakukan Nika Ratama mengenai pengembangan aplikasi Android dengan integrasi algoritma *Rivers Code* 4 dan *Least significant bit* untuk keamanan data. Algoritma RC4 digunakan untuk metode enkripsi data dengan *stream cipher* yang sederhana, sehingga dapat menghasilkan pola data yang aman. Algoritma LSB digunakan untuk menyisipkan data yang telah di enkripsi ke dalam citra digital tanpa menyebabkan perubahan yang signifikan. Penelitian tersebut mengamankan *file* dalam bentuk *.pdf, *.docx, *.xls, dan *.txt. Hasil penelitian menunjukkan kombinasi antara teknik kriptografi dan steganografi efektif dalam mengamankan data-data rahasia [1] .

2. Caesar Cipher

Caesar Cipher adalah sebuah teknik enkripsi yang menggunakan metode substitusi untuk mengamankan pesan [15]. Caesar Cipher merupakan salah satu metode kriptografi yang berfungsi untuk melindungi data dengan mengenkripsi informasi agar tidak dapat dengan mudah dipahami oleh pihak yang lain. Algoritma ini, bekerja dengan menggantikan setiap huruf pada teks asli (*plaintext*) dengan huruf lain yang posisinya bergeser sejumlah tertentu dalam urutan alfabet, sesuai dengan kunci yang diberikan. Proses pembentukan *ciphertext* melibatkan beberapa tahapan dimulai dengan menentukan jumlah pergeseran karakter yang akan digunakan untuk mengubah *plaintext* menjadi *ciphertext*. Mengganti setiap karakter pada *plaintext* dengan karakter yang telah digeser berdasarkan nilai pergeseran yang ditentukan. Misalnya, jika pergeseran yang digunakan adalah 3, maka huruf A akan diganti menjadi huruf D, huruf B menjadi huruf E, dan seterusnya [16]. Hal tersebut ditunjukkan pada Gbr 1. Untuk baris pertama menunjukkan huruf asli dan baris kedua menunjukkan hasil pergeseran huruf sebanyak tiga kali.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Gbr. 1 Skema Caesar Cipher

Untuk setiap perubahan *plaintext* menjadi *ciphertext* dapat melalui perhitungan enkripsi:

$$C = E(k, p) = (p + k)\ mod\ 26$$

Kemudian untuk melakukan perubahan dari *ciphertext* menjadi *plaintext* melalui perhitungan dekripsi, untuk nilai k berasal dari jumlah pergeseran yang dilakukan dalam rentang 1 hingga 26 [17].

$$p = D\ (k, C) = (C - k)\ mod\ 26$$

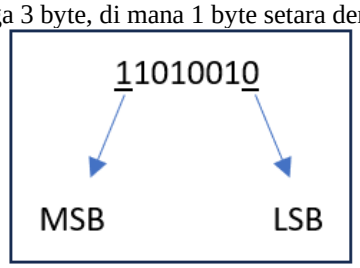
Sebagai contoh pada Gbr 2, *plaintext* yang akan di enkripsi yaitu ‘KEAMANAN DATA’, sehingga hasil *ciphertext* yang diperoleh adalah’NHDPDQDQ GDWD’. Proses ini menggambarkan cara kerja Caesar Cipher dalam mengubah *plaintext* menjadi *ciphertext* dengan menggunakan kunci nilai pergeseran yang telah ditentukan sebelumnya.

K	E	A	M	A	N	A	N		D	A	T	A
N	H	D	P	D	Q	D	Q		G	D	W	D

Gbr. 2 Percobaan Proses Caesar Cipher

3. *Least significant bit*

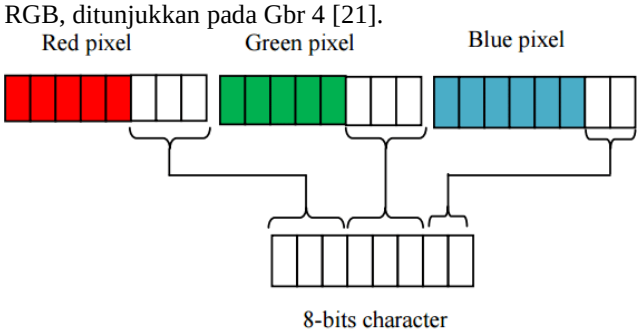
Least significant bit atau LSB merupakan metode yang sering digunakan untuk proses enkripsi dan dekripsi informasi yang bersifat rahasia [18]. *Least significant bit* menjadi salah satu algoritma menyisipkan pesan ke dalam gambar pada teknik steganografi. Metode ini bekerja dengan cara mengganti bit terakhir dari kode biner gambar dengan kode biner pesan [19]. Dalam teknik penyisipan LSB, diterapkan pada citra digital seperti *covertext*. Setiap piksel dalam *file* memiliki ukuran antara 1 hingga 3 byte, di mana 1 byte setara dengan 8 bit.



Gbr. 3 Perbedaan MSB dan LSB

Pada *byte* dengan nilai 11010010, bit pertama adalah MSB, dan bit terakhir adalah LSB. Bit yang paling tepat untuk dimodifikasi adalah bit LSB karena bit ini mudah diubah sedikit, baik menjadi lebih tinggi atau lebih rendah dari nilai sebelumnya. Dengan LSB, perubahan yang dilakukan tidak akan menimbulkan kecurigaan bagi manusia dan mudah untuk diterapkan [20]. Dalam penerapannya pada citra warna RGB, menggunakan bit LSB dari setiap saluran warna (*Red*, *Green*, *Blue*) yang masing-masing bernilai 8-bit untuk menyisipkan pesan tersembunyi. Proses perubahan yang terjadi pada bit LSB tidak dapat secara langsung diketahui oleh manusia, sehingga data dapat disisipkan secara aman tanpa memengaruhi kualitas visual gambar. Misalnya, pesan teks yang terdiri dari 8-bit dipecah menjadi tiga bagian dalam RGB. Urutan 8-bit yang diterapkan dalam proses penyisipan untuk

dapat mengembalikan pesan rahasia dari citra sampul warna RGB, ditunjukkan pada Gbr 4 [21].



Gbr. 4 LSB pada gambar sampul RGB

III.METODE PENELITIAN

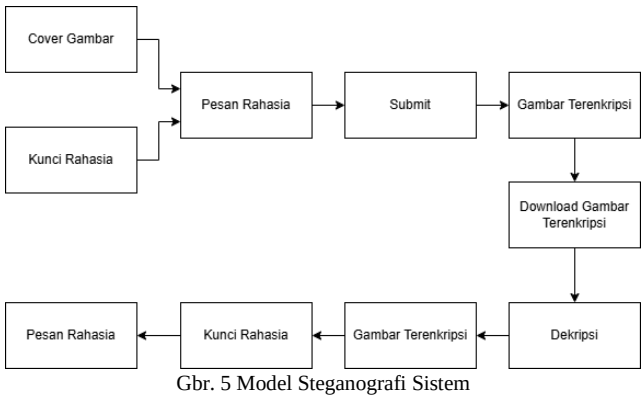
Penelitian ini dilakukan melalui beberapa tahap utama, yaitu tahap analisis kebutuhan, desain sistem, implementasi, dan pengujian. Penelitian ini berfokus pada pengembangan aplikasi mobile berbasis Android yang mengintegrasikan algoritma Caesar Cipher untuk kriptografi dan *Least significant bit* (LSB) untuk steganografi.

1. Analisis Kebutuhan

Tahap pertama dari penelitian ini adalah analisis kebutuhan. Pada tahap ini, kebutuhan sistem diidentifikasi untuk memastikan aplikasi yang dikembangkan memiliki fitur yang sesuai dengan tujuan penelitian. Aplikasi yang dirancang harus mampu mengenkripsi pesan menggunakan algoritma Caesar Cipher, menyisipkan pesan terenkripsi ke dalam citra digital menggunakan algoritma *Least significant bit* (LSB), dan mengekstrak pesan tersebut dari gambar serta mendekripsinya. Hasil dari analisis kebutuhan ini adalah daftar fitur utama yang harus dimiliki aplikasi, termasuk kemampuan untuk melakukan enkripsi, penyisipan pesan, dekripsi, dan pengambilan pesan.

2. Desain Sistem

Tahapan selanjutnya adalah desain sistem, di mana struktur aplikasi dan alur kerja dirancang untuk memastikan integrasi algoritma dapat berjalan dengan baik. Alur sistem melibatkan beberapa proses utama, dimulai dari enkripsi pesan menggunakan algoritma Caesar Cipher, kemudian dilanjutkan dengan penyisipan pesan yang telah terenkripsi ke dalam gambar menggunakan algoritma LSB. Desain sistem ini memastikan bahwa setiap langkah saling terhubung secara efisien.



Gbr. 5 Model Steganografi Sistem

Aplikasi dirancang memiliki antarmuka pengguna yang sederhana dan intuitif. Pada menu utama, terdapat dua fungsi utama: “Encrypt”, yang digunakan untuk mengenkripsi pesan dan menyisipkannya ke dalam gambar, serta “Decrypt”, yang digunakan untuk mengekstrak pesan tersembunyi dari gambar dan mendekripsinya.

3. Implementasi

Setelah desain sistem selesai, langkah berikutnya adalah implementasi. Pada tahap ini, algoritma Caesar Cipher dan LSB diimplementasikan terlebih dahulu menggunakan bahasa pemrograman Python. Implementasi awal ini bertujuan untuk menguji fungsi utama algoritma sebelum integrasinya ke dalam aplikasi Android.

Algoritma Caesar Cipher digunakan untuk mengenkripsi pesan dengan menggantikan setiap huruf dalam *plaintext* berdasarkan pergeseran kunci yang ditentukan pengguna. Proses ini menghasilkan *ciphertext* yang tidak mudah dimengerti oleh pihak ketiga. Kode implementasi algoritma Caesar Cipher sebagai berikut:

```
def encrypt_message(message, key):
    """Mengenkripsi pesan menggunakan Caesar Cipher."""
    return ''.join(chr((ord(char) - ord('A') + key) % 26 + ord('A')) if char.isupper() else char for char in message)
```

Setelah digeser sesuai dengan *key* yang diinputkan *user*, tiap karakter kemudian akan disubstitusikan ke dalam kamus enkripsi kustom sehingga pesan akan semakin sulit untuk dipecahkan.

```
def create_shifted_substitution(key):
    original_substitution = {
        'A': 'Batu', 'B': 'Lebah', 'C': 'Kaca', 'D': 'Lada', 'E': 'Lelah', 'F': 'Info',
        'G': 'Laga', 'H': 'Bahu', 'I': 'Diri', 'J': 'Baja', 'K': 'Luka', 'L': 'Pulau',
        'M': 'Lama', 'N': 'Dunia', 'O': 'Solo', 'P': 'Tepi', 'Q': 'Taqwa', 'R': 'Bara',
        'S': 'Masa', 'T': 'Kota', 'U': 'Kutu', 'V': 'Lava', 'W': 'Mawar', 'X': 'Pixel',
        'Y': 'Daya', 'Z': 'Azan',
        'a': 'batu', 'b': 'lebah', 'c': 'kaca', 'd': 'lada', 'e': 'lelah', 'f': 'info',
        'g': 'laga', 'h': 'bahu', 'i': 'diri', 'j': 'baja', 'k': 'luka', 'l': 'pulau',
        'm': 'lama', 'n': 'dunia', 'o': 'solo', 'p': 'tepi', 'q': 'taqwa', 'r': 'bara',
        's': 'masa', 't': 'kota', 'u': 'kutu', 'v': 'lava', 'w': 'mawar', 'x': 'pixel',
        'y': 'daya', 'z': 'azan',
        ' ': 'spasi',
        '.': 'titik',
        ',': 'koma' }
```

Selanjutnya, algoritma LSB digunakan untuk menyisipkan pesan terenkripsi ke dalam citra digital. Pesan dienkripsi terlebih dahulu, kemudian diubah menjadi representasi biner dan disisipkan ke dalam *Least significant bit* dari piksel gambar. Proses ini dilakukan menggunakan pustaka Python seperti PIL untuk memanipulasi piksel gambar. Berikut adalah kode untuk penyisipan pesan:

```
def encode_image(image_name, message, output_image_name):
    """Menyisipkan pesan ke dalam gambar menggunakan algoritma LSB."""
```

```
    from PIL import Image
    image = Image.open(image_name).convert('RGB')
    message += "$$"  # Penanda akhir pesan
    binary_message = ''.join(format(ord(char), '08b') for char
in message)
    pixels = image.load()
    idx = 0
    for y in range(image.height):
        for x in range(image.width):
            if idx < len(binary_message):
                r, g, b = pixels[x, y]
                pixels[x, y] = (r & ~1 | int(binary_message[idx]),
g, b)
                idx += 1
    image.save(output_image_name, 'PNG')
    return "Pesan berhasil disembunyikan."
```

Tahap implementasi ini juga mencakup proses penguraian pesan dari gambar untuk memastikan pesan yang disisipkan dapat diekstraksi dan didekripsi kembali ke bentuk aslinya.

```
def decrypt_message(encrypted_message, key):
    """Mendekripsi pesan yang dienkripsi."""
    substitution_dict = create_shifted_substitution(key)
    # Buat dictionary terbalik untuk dekripsi
    reverse_dict = {v: k for k, v in substitution_dict.items()}

    # Split pesan terenkripsi menjadi kata-kata
    words = encrypted_message.strip().split(' ')
    decrypted = []

    for word in words:
        if word in reverse_dict:
            decrypted.append(reverse_dict[word])
        else:
            decrypted.append(word)

    return ''.join(decrypted)
```

Fungsi decrypt_message menerima pesan terenkripsi dan kunci sebagai input, kemudian menggunakan kamus substitusi yang digeser berdasarkan kunci untuk membuat kamus terbalik. Pesan terenkripsi dipecah menjadi kata-kata, kemudian setiap kata dicocokkan dengan kamus terbalik untuk mengembalikan karakter aslinya. Hasil akhirnya adalah pesan yang telah didekripsi kembali menjadi teks asli.

4. Pengujian

Tahap terakhir dari metode penelitian ini adalah pengujian. Pengujian dilakukan untuk memastikan bahwa algoritma Caesar Cipher dan LSB dapat bekerja secara efisien dalam melindungi pesan rahasia. Validasi dilakukan untuk memastikan hasil enkripsi Caesar Cipher dapat didekripsi dengan benar. Selain itu, proses penyisipan pesan ke dalam gambar diuji untuk mengevaluasi kualitas gambar setelah dilakukan steganografi. Pengujian melibatkan analisis visual pada gambar hasil steganografi untuk memastikan kualitasnya tidak mengalami penurunan yang signifikan.

Pengujian dilakukan dengan menggunakan dua metode utama yaitu *Mean Squared Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR). MSE digunakan untuk mengukur perbedaan antara gambar asli dengan gambar hasil steganografi. Nilai MSE yang lebih rendah menunjukkan bahwa gambar hasil steganografi memiliki kualitas yang mendekati gambar asli. PSNR digunakan untuk mengukur kualitas visual gambar hasil steganografi. Nilai PSNR yang lebih tinggi menunjukkan kualitas gambar hasil steganografi yang lebih baik dan sedikitnya distorsi yang terjadi.

IV.HASIL DAN PEMBAHASAN

Hasil dari penelitian ini berisikan tampilan dari aplikasi PiGANO penerapan dari algoritma Caesar Cipher dan *Least significant bit* untuk menyembunyikan pesan di dalam gambar. Adapun tampilan awal aplikasi PiGANO dimuat pada Gbr 6.

Gbr. 6 Tampilan Awal Aplikasi PiGANO

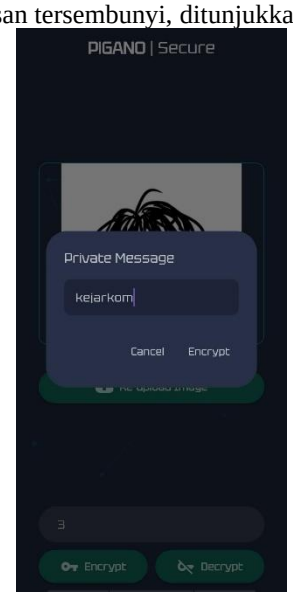
Pengguna dapat menekan tombol “Coba Sekarang!” yang kemudian akan diarahkan pada halaman utama. Halaman tersebut berisikan hal-hal yang harus diisi oleh pengguna, meliputi unggah gambar, memasukkan kunci sebanyak 1-8 digit, melakukan proses enkripsi dan dekripsi yang berada di Gbr 7.

Gbr. 7 Tampilan Halaman Utama PiGANO

Pada halaman tersebut, pengguna diberikan opsi untuk memasukkan gambar yang ingin diunggah beserta dengan kunci yang diinginkan. Proses ini dapat ditinjau pada Gbr 8.

Gbr. 8 Tampilan Menginputkan Gambar dan Kunci

Setelah itu, pengguna dapat melakukan proses enkripsi dengan menekan tombol "Encrypt". Ketika tombol tersebut ditekan, akan muncul *pop-up* yang meminta pengguna untuk memasukkan pesan tersembunyi, ditunjukkan pada Gbr 9.



Gbr. 9 Tampilan Menginputkan Pesan Enkripsi

Setelah pesan dimasukkan, pengguna akan diarahkan ke halaman baru berupa tampilan gambar hasil enkripsi pada Gbr 10. Bukan hanya itu saja, di halaman tersebut menampilkan pesan yang disembunyikan "kejarkom" dan hasil pesan yang telah diproses menjadi *ciphertext* "dunia bahu lama lada kutu duni..". Selain itu, dilakukan pengujian dengan parameter nilai MSE (*Mean Squared Error*) dan PSNR (*Peak Signal-to-Noise Ratio*) dari gambar hasil enkripsi.

Mean Squared Error (MSE) digunakan untuk menghitung rata-rata kuadrat kesalahan antara piksel pada citra asli dan piksel pada citra hasil steganografi. Nilai MSE yang lebih kecil menunjukkan perbedaan yang lebih kecil antara cover image dan stego image, yang berarti kualitas citra hasil steganografi lebih mendekati citra asli. Rumus untuk menghitung MSE yaitu:

$$MSE = \sum \frac{(y(predicted) - y(actual)^2)}{N} \quad (1)$$

Peak Signal-to-Noise Ratio (PSNR) digunakan untuk mengukur kualitas citra dalam satuan desibel (dB). PSNR menunjukkan rasio antara energi sinyal maksimum (intensitas piksel tertinggi) dan tingkat gangguan atau distorsi yang terjadi pada citra. Rumus untuk menghitung PSNR dinyatakan sebagai berikut:

$$10 \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \quad (2)$$

Perolehan nilai MSE pada gambar tersebut sebesar 0.000142 sedangkan untuk nilai PSNR sebesar 86.603453.

Gbr. 10 Tampilan Hasil Enkripsi

Setelah itu, pengguna dapat melakukan proses dekripsi untuk mengakses pesan yang disembunyikan. Proses ini dilakukan dengan menggunggah gambar hasil enkripsi dan memasukkan kunci yang sama dengan proses enkripsi, yang menekan tombol "Decrypt". Kemudian, pengguna akan diarahkan ke halaman hasil dekripsi, yang menampilkan gambar dan pesan hasil dekripsi, ditunjukkan pada Gbr 11.

Gbr. 11 Tampilan Hasil Dekripsi

Dilakukan beberapa kali pengujian pada aplikasi PiGANO dengan menambahkan pesan yang ingin disembunyikan pada sebuah gambar. Diperoleh *ciphertext* pada setiap pesan yang disembunyikan serta *quality parameters* untuk mengukur tingkat kesalahan dari gambar asli dengan gambar enkripsi

(MSE) dan mengukur kualitas gambar hasil enkripsi (PSNR), ditunjukkan pada Tabel I.

TABEL I
HASIL PENGUJIAN APLIKASI

Foto	Pesan	Key	Ciphert-ext	*Quality Parameters*	
				MSE	**PSNR**
	kejarkom	3	Dunia bahu lama lada kutu duni..	0.000142	86.603453
	Lena	3	Solo bahu taqwa lada	**0.000003**	**103.695638**
	Lisa	3	Solo pulau lava lada	0.000041	92.042658

V.KESIMPULAN

Berdasarkan pengujian yang telah dilakukan melalui perhitungan nilai MSE (*Mean Squared Error*) dan PSNR (*Peak Signal-to-Noise Ratio*), menunjukkan bahwa nilai PSNR yang lebih tinggi menandakan kualitas rekonstruksi citra yang lebih baik, karena perbedaan atau *noise* antara citra asli dan hasil rekonstruksi semakin berkurang. Sementara itu, nilai MSE yang rendah menunjukkan adanya kesalahan yang minimal antara citra asli dan hasil rekonstruksi, yang mengindikasikan bahwa algoritma atau metode yang diterapkan dalam pengolahan citra bekerja dengan baik. Hasil dari MSE yang rendah dan PSNR yang tinggi menunjukkan bahwa aplikasi ini dapat mengenkripsi serta menyembunyikan pesan dalam gambar tanpa mengurangi kualitas visual secara signifikan, sehingga perubahan yang terjadi tidak terlihat oleh indra penglihatan.. Ini membuktikan bahwa kombinasi teknik kriptografi dan steganografi pada algoritma Caesar Cipher dan *Least significant bit* memberikan tingkat keamanan ganda yang sangat efektif dalam menjaga kerahasiaan pesan yang disembunyikan pada media gambar.

VI.DAFTAR PUSTAKA

[1] N. Ratama and M. Munawaroh, "Implementasi Metode Kriptografi dengan Menggunakan Algoritma RC4 dan Steganografi *Least significant bit* Dalam Mengamankan Data Berbasis Android," *J. Media Inform. Budidarma*, vol. 6, no. 2, p. 1272, 2022, doi: 10.30865/mib.v6i2.3902.

[2] M. B. Yel and M. K. M. Nasution, "Keamanan Informasi Data Pribadi Pada Media Sosial," *J. Inform. Kaputama*, vol. 6, no. 1, pp. 92–101, 2022, doi: 10.59697/jik.v6i1.144.

[3] I. U. W. Mulyono, Y. Kusumawati, and N. K. Ningrum, "Analisa Visual Citra Hasil Kombinasi Steganografi dan Kriptografi Berbasis *Least significant bit* Dalam Cipher," *J. Masy. Inform.*, vol. 14, no. 1, pp. 16–28, 2023, doi: 10.14710/jmasif.14.1.51484.

[4] A. A. Permana, "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android," *J. Al-AZHAR Indones. SERI SAINS DAN Teknol.*, vol. 4, no. 3, p. 110, 2018, doi: 10.36722/sst.v4i3.280.

[5] D. Pradeka, "Implementasi Aplikasi Kriptografi Berbasis Android Menggunakan Metode Substitusi dan Permutasi," Search Inform. Sci. Entrep. Appl. Art Res. Humanism, vol. 18, no. 1, Art. no. 1, Apr. 2019, doi: 10.37278/insearch.v18i1.148.

[6] Y. D. Putri *et al.*, "Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance Application of Caesar Cipher Criptography in Freelance," *J. Inform. dan Komputer) p-ISSN*, vol. 2, no. 2, pp. 87–94, 2019.

[7] N. A. Ramadhani and I. Susilawati, "Penerapan Steganografi untuk Penyisipan Pesan Teks pada Citra Digital dengan Menggunakan Metode *Least significant bit*," *J. Multimed. Artif. Intell.*, vol. 4, no. 1, pp. 21–27, 2020.

[8] A. R. Hakim and W. M. Baihaqi, "KOMPUTA : Jurnal Ilmiah Komputer dan Informatika TIKET PESAWAT BERBASIS WEB KOMPUTA : Jurnal Ilmiah Komputer dan Informatika," vol. 12, no. 2, pp. 50–58, 2023.

[9] F. Yanti and K. Budayawan, "Implementasi Steganografi Menggunakan Metode *Least significant bit* (LSB) dalam Pengamanan Informasi pada Citra Digital," *Voteteknika (Vocational Tek. Elektron. dan Inform.*, vol. 11, no. 1, p. 63, 2023, doi: 10.24036/voteteknika.v11i1.121968.

[10] D. Laoli and B. Sinaga, "Desimeri Laoli 1 , Bosker Sinaga 2 [Penerapan Algoritma Hill Cipher Dan *Least significant bit* (LSB) Untuk Pengamanan Pesan," vol. 1, no. 2, pp. 30–40, 2018.

[11] A. W. Laksono, S. Suhada, and A. Zakaria, "Implementasi Metode *Least significant bit* (Lsb) Dalam Teknik Steganografi Pada Citra Digital Menggunakan Matlab," vol. 4, no. 1, 2024.

[12] M. Basri and M. Fadhlil Gushari, "Penerapan Steganografi Gambar Berwarna Pada Delapan Image Cover Menggunakan Metode Lsb," *J. Sintaks Log.*, vol. 1, no. 3, pp. 153–158, 2021, doi: 10.31850/jsilog.v1i3.1128.

[13] Saifuddin, A. Rakhmadi Mido, and E. Ujianto, "Perancangan Aplikasi Steganografi Menggunakan Metode Discrete Cosine Transformation berbasis Android," *J. Ilm. Komput.* , vol. 16, no. 1, pp. 25–36, 2020.

[14] N. E. Saragih and F. Harahap, "Menggunakan Algoritma One Time Pad Implementation of One Time Pad Algorithm in Android Diary Application," *SNITT- Politek. Negeri Balikpapan* , vol. 4, no. 7, pp. 316–320, 2020.

[15] R. Febrianingsih, A. Hafiz, and M. Informatikan, "Jurnal Informasi Dan Komputer Vol : 7 No : 2 Thn .: 2019 IMPLEMENTASI KRIPTOGRAFI BERBASIS CAESAR CHIPER UNTUK Jurnal Informasi Dan Komputer Vol : 7 No : 2 Thn .: 2019," *Anal. Infrastruktur Teknol. Inf. Menggunakan Framew. Cobit 4.1*, vol. Vol :7, pp. 81–86, 2019.

[16] R. W. Asiani and I. Yanti, "Penerapan Kriptografi Caesar Cipher Dan Hill Cipher dalam Pengiriman Pesan Rahasia Sebagai Media Pembelajaran Matematika Realistik Pada Materi Modulo.pdf," *Baitul 'Ulum J. Ilmu Perpust. dan Inf.*, vol. 6, no. 1, pp. 79–97, 2022.

[17] N. C. Safitri and A. Prihanto, "Modifikasi Cipher Kriptografi Caesar yang Dapat Dibaca dengan Menggunakan Kamus Bahasa Indonesia," *J. Informatics Comput. Sci.*, vol. 1, no. 01, pp. 34–41, 2019, doi: 10.26740/jinacs.v1n01.p34-41.

[18] Adiria, "Analisis dan perancangan aplikasi steganografi pada citra digital menggunakan metode lsb (*Least significant bit*)," *IKRAM J. Ilmu Komput. AI Muslim*, vol. III, no. 1, pp. 1–5, 2024.

[19] Z. Niswati, "Steganografi Berbasis *Least significant bit* (Lsb) Untuk Menyisipkan Gambar Ke Dalam Citra Gambar," *Fakt. Exacta*, vol. 5, no. 2, pp. 181–191, 1979, [Online]. Available: https://journal.lppmunindra.ac.id/index.php/Faktor_Exacta/article/download/194/185

[20] C. Nugroho and Muslihudin, "Steganografi Pada Pengiriman Teks Pesan Gambar dengan Metode *Least significant bit* & Steghide," *J. Ilmu Siber*, vol. 1, no. 3, pp. 44–47, 2022, [Online]. Available: https://jurnal.unsia.ac.id/index.php/jis/article/view/54%0Ahttps://jurnal.unsia.ac.id/index.php/jis/article/download/54/40

[21] K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E. S. M. El-Rabaie, and G. M. El-Banby, "High security data hiding using image cropping and LSB *least significant bit* steganography," *Colloq. Inf. Sci. Technol. Cist*, vol. 0, no. October 2019, pp. 400–404, 2016, doi: 10.1109/CIST.2016.7805079.